F2 : Eléments de correction

ex1 q1) On a $x \equiv 0\ [4]$ ou $x \equiv 1\ [4]$ ou $x \equiv 2\ [4]$ ou $x \equiv -1\ [4]$

D'où $x^2 \equiv 0\ [4]$ ou $x^2 \equiv 1\ [4]$ ou $x^2 \equiv 0\ [4]$ ou $x^2 \equiv 1\ [4]$.

Par conséquent les restes possibles de $X = x^2$ dans la division par 4 sont 0 ou 1.

q2) On a $x \equiv 0\ [3]$ ou $x \equiv \pm 1 [3]$ d'où $x^2 \equiv 0\ [3]$ ou $x^2 \equiv 1\ [3]$.

Par conséquent les restes possibles de $X = x^2$ dans la division par 3 sont 0 ou 1.

ex2 D'après ex1, (q1), on a $n^2 \equiv 0$ ou $1\ [4]$ donc $n^2+1 \equiv 1$ ou $2\ [4]$.

En aucun cas on ne peut avoir n^2+1 congru à 0 modulo 4 donc 4 ne peut diviser aucun nombre de la forme n^2+1.

ex3 On a $7 \equiv -1\ [8]$ donc $7^n \equiv (-1)^n\ [8]$ donc $7^n+1 \equiv (-1)^n+1\ [8]$.

Si n est impair on a $7^n+1 \equiv -1+1\ [8]$ donc $8 \mid 7^n+1$.

Si n est pair on a $7^n+1 \equiv (-1)^{2k}+1\ [8]$ donc $7^n+1 \equiv 2\ [8]$ et donc le reste de la division de 7^n+1 par 8 est 2.

ex4 On a $\mathrm{pgcd}(6,9) = 3$ donc $S \Rightarrow \begin{cases} x \equiv 4 \bmod 3 \\ x \equiv 7 \bmod 3 \end{cases} \Rightarrow 4 \equiv 7\ [3]$

et ceci est vrai donc le système S admet des solutions.

Pour trouver une solution particulière x_0 de S on regarde le système S' déduit de S, avec $S' \begin{cases} x \equiv 4 \bmod 2 \\ x \equiv 7 \bmod 3 \end{cases}$ qui lui admet la solution particulière $x_0 = 4 \times 3 + 7 \times (-2) = -2$ déduite de la relation de Bezout $3 - 2 = 1$ (possible vu que $\mathrm{pgcd}(2,3) = 1$)

En effet si $3u + 2v = 1$ on a $\begin{cases} 3u \equiv 1\ [2] \\ 3u \equiv 0\ [3] \end{cases}$ et $\begin{matrix} 2v \equiv 0\ [2] \\ 2v \equiv 1\ [3] \end{matrix}$

donc $4 \times 3u + 7 \times 2v = x_0$ vérifie bien $\begin{cases} x_0 \equiv 4\ [2] \\ x_0 \equiv 7\ [3]. \end{cases}$

Comme expliqué dans le cours, cette solution particulière x_0 est aussi une solution particulière de S si on a fait attention à ne pas simplifier les valeurs 4 et 7 mod 2, respectivement mod 3 mais si on les garde telles quelles.

En effet $\begin{cases} -2 \equiv 4 \ [6] \\ -2 \equiv 7 \ [9] \end{cases}$. Maintenant $S \Leftrightarrow \begin{cases} x \equiv x_0 \ [6] \\ x \equiv x_0 \ [9] \end{cases}$

$\Leftrightarrow \begin{cases} 6 \mid x - x_0 \\ 9 \mid x - x_0 \end{cases} \Leftrightarrow ppcm(6,9) = 18 \mid x - x_0 \Leftrightarrow x \equiv x_0 \ [18]$

$\Leftrightarrow x \equiv -2 \ [18]$ qui est la solution finale de S, ou que l'on a procédé par équivalence.

ex5

q1) On a $x \equiv \pm 1 \ [p] \Rightarrow x^2 \equiv 1 \ [p]$ clairement

Reciproquement $x^2 \equiv 1 \ [p] \Leftrightarrow p \mid x^2 - 1 \Leftrightarrow p \mid (x-1)(x+1)$

$\Leftrightarrow p \mid x - 1$ ou $p \mid x + 1 \Leftrightarrow x \equiv 1 \ [p]$ ou $x \equiv -1 \ [p]$.

lemme d'Euclide

q2) Pour simplifier le équations du système on cherche des inverses de 2 modulo 5 et de 4 modulo 7. Ceux-ci sont faciles à trouver car $2 \times 3 = 6 \equiv 1 \ [5]$ et $4 \times 2 = 8 \equiv 1 \ [7]$.

On sait alors que $2x \equiv 3 \ [5] \Leftrightarrow 3 \cdot 2x \equiv 3 \cdot 3 \ [5] \Leftrightarrow$ $6x \equiv 9 \ [5] \Leftrightarrow x \equiv 4 \ [5]$ et que $4x \equiv 3 \ [7] \Leftrightarrow 2 \cdot 4x \equiv 2 \cdot 3 \ [7]$

$\Leftrightarrow 8x \equiv 6 \ [7] \Leftrightarrow x \equiv 6 \ [7]$.

Le système de départ est alors équivalent à $S \begin{cases} x \equiv 4 \ [5] \\ x \equiv 6 \ [7] \end{cases}$

Comme $pgcd(5,7) = 1$ on a une relation de Bezout entre 5 et 7, par exemple $3 \times 5 - 2 \times 7 = 1$ qui nous permet de donner une solution particulière $x_0 = 6\times 3\times 5 - 4\times 2\times 7 = 34$ pour S.

Alors $S \Leftrightarrow \begin{cases} x \equiv x_0 \ [5] \\ x \equiv x_0 \ [7] \end{cases} \Leftrightarrow \begin{cases} 5 \mid x - x_0 \\ 7 \mid x - x_0 \end{cases} \Leftrightarrow ppcm(5,7) = 35 \mid x - x_0$

$\Leftrightarrow x \equiv x_0 \ [35] \Leftrightarrow x \equiv 34 \ [35] \Leftrightarrow x \equiv -1 \ [35]$, qui est la solution finale du système de départ.

ex6 q1) On a $pgcd(9n+15, 4n+7) = pgcd(9n+15 - 2(4n+7), 4n+7) =$
$= pgcd(n+1, 4n+7) = pgcd(n+1, 4n+7 - 4(n+1)) = pgcd(n+1, 3) = d$

Si $3 \mid n+1$ alors $pgcd(n+1,3) = 3$ et si $3 \nmid n+1$, $pgcd(n+1,3) = 1$.
On peut dire aussi que si $n \equiv -1 \ [3]$, $d = 3$ et si $n \equiv 0$ ou $1 \ [3]$ alors $d = 1$.

On peut remarquer aussi que $d \mid 4(9n+15) - 9(4n+7) = -3$.
Comme $3 \mid 9n+15$ on a $d = 3$ si $3 \mid 4n+7$ càd $3 \mid n+1$.

q2) Soit $p > 0$ un nombre premier tel que $p \mid n^2$ et $p \mid 2n+1$.
Comme $p \mid n^2$ on a $p \mid n$ d'après le lemme d'Euclide.
On a encore $p \mid 2n$ donc $p \mid 2n+1-2n = 1$. Ceci étant impossible on en déduit que n^2 et $2n+1$ n'ont aucun facteur premier en commun donc que $pgcd(n^2, 2n+1) = 1$.

ex7 On écrit $n = \overline{abcdef} = \overline{abc} \cdot 1000 + \overline{def}$ et on a $6n + 21 = \overline{def} \cdot 1000 + \overline{abc}$. Notons $x = \overline{abc}$ et $y = \overline{def}$ et résolvons $\begin{cases} n = x \cdot 1000 + y \\ 6n + 21 = y \cdot 1000 + x \end{cases}$ On a alors

$6000x + 6y + 21 = 1000y + x$ d'où $5999x + 21 = 994y$
$\Leftrightarrow 3 = -857x + 142y$ et $pgcd(857, 142) = 1$ donc il y a des solutions dans $\mathbb{Z}$.

On écrit ensuite $857 = 142 \times 6 + 5$

$142 = 5 \times 28 + 2$

$5 = 2 \times 2 + 1$ (l'algorithme d'Euclide pour 857 et 142, qui permet, en le remontant, de trouver une relation de Bezout entre 857 et 142)

càd $1 = 5 - 2 \times 2$

$1 = 5 - (142 - 5 \times 28) \times 2 = 5 \times 57 - 142 \times 2$

$1 = (857 - 142 \times 6) \times 57 - 142 \times 2 = 857 \times 57 - 142 \times 344$

Alors $3 = 857 \times 171 - 142 \times 1032 = -857x + 142y$

On en déduit $857(171 + x) = 142(y + 1032)$ donc

$142 \mid 857(171+x)$. D'après le lemme de Gauss, vu que $\text{pgcd}(142, 857) = 1$ on a $142 \mid 171 + x$ donc $171 + x = 142k$ avec $k \in \mathbb{Z}$. Par conséquent $y + 1032 = 857k$ et toutes les solutions sont $x = 142k - 171$ et $y = 857k - 1032$

(Vérification éventuelle : $-857(142k - 171) + 142(857k - 1032) =$

$= -857 \cdot 142k + 857 \cdot 171 + 142 \cdot 857k - 142 \cdot 1032 = 3$).

On cherche parmi $142k - 171$ et $857k - 1032$ des solutions à 3 chiffres. On doit prendre alors $k = 2$ et $x = 113$, $y = 682$

On vérifie bien que $6n + 21 = 682\,113$ lorsque $n = 113\,682$.

Ex 8 q1) On voit que $P(n) = n(n-1) + 41$ donc si $n = 41$ ou $n = 42$

on a $P(41) = 41 \cdot 40 + 41 = 41^2$ non premier et

$P(42) = 42 \cdot 41 + 41 = 43 \cdot 41$ non premier.

Ce qui est impressionnant ici, c'est que

$P(0) = 41$, $P(1) = 41$, $P(2) = 43$, $P(3) = 47$, $P(4) = 53$

$P(5) = 61$, $P(6) = 71$, $P(7) = 83$, $P(8) = 97$, $P(9) = 113$

$P(10)=131$, $P(11)=151$, $P(12)=173$, $P(13)=197$, $P(14)=223$
$P(15)=251$, $P(16)=281$, $P(17)=313$, $P(18)=347$, $P(19)=383$
$P(20)=421$, $P(21)=461$, $P(22)=503$, $P(23)=547$, $P(24)=593$
$P(25)=641$, $P(26)=691$, $P(27)=743$, $P(28)=797$, $P(29)=853$
$P(30)=911$, $P(31)=971$, $P(32)=1033$, $P(33)=1097$, $P(34)=1163$
$P(35)=1231$, $P(36)=1301$, $P(37)=1373$, $P(38)=1447$, $P(39)=1523$
et $P(40)=1601$ sont tous des nombres premiers !!!

q2) On a $n^2-n+41 = n^2-n-2+43 = (n-2)(n+1)+43$

Ce nombre est divisible par 43 pour tout $n=43k+2$ ou $n=43k-1$, $k\in\mathbb{N}$. Il existe donc une infinité de n tels que $43 \mid P(n)$.

ex9 q1) On a $(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1} a^{k+1}b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} =$

$= \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} = a^n + \sum_{k=1}^{n-1} a^k b^{n-k} - \sum_{k=1}^{n-1} a^k b^{n-k} - b^n =$

$= a^n - b^n \quad \forall\, a,b\in\mathbb{R},\ n\in\mathbb{N}^*.$

q2) "$\Leftarrow$" Si $m \mid n$ on a $n=ml$, $l\in\mathbb{N}$ et $a^n-1=(a^m)^l-1 \overset{\text{d'après q1}}{=} (a^m-1)\sum_{k=0}^{l-1}(a^m)^k$ si $l\geq 1$. Si $l=0$ on a $m=n=0$ et $a^m-1=0$ divise $a^n-1=0$. Dans tous les cas $a^m-1 \mid a^n-1$.

"$\Rightarrow$" Si a^m-1 divise a^n-1 on écrit la division euclidienne de n par $m\neq 0$: $n=mq+r$ avec $0\leq r<m$.
Alors $a^n-1 = a^{mq+r}-1 = a^{mq+r}-a^r+a^r-1 =$
$= a^r(a^{mq}-1)+a^r-1$ (*). D'après le sens "$\Leftarrow$" ci-dessus, vu que $m \mid mq$, on a que $a^m-1 \mid a^{mq}-1$, et comme $a^m-1 \mid a^n-1$

on en déduit que $a^m-1 \mid a^r-1$. Or $a^r < a^m$ donc $a^r-1 < a^m-1$. Si $r>0$, $a^r-1>0$ (vu que $a \geq 2$) donc a^m-1 ne peut pas diviser a^r-1 qui lui est inférieur.

Alors $r=0$ et $n=mq$ est divisible par m.

Si $m=0$ on a $a^m-1=0$. Comme $a^m-1 \mid a^n-1$ on a $a^n-1=0$ aussi donc $a^n=1$ et vu que $a \neq 1$ on a $n=0$ divisible par $m=0$.

(*) Remarque : Si $n=mq+r$ est la DE (division euclidienne) de n par m alors $a^n-1=(a^m-1)Q+a^r-1$ est la DE de a^n-1 par a^m-1. Donc l'algorithme d'Euclide entre n et m implique l'algorithme d'Euclide entre a^n-1 et a^m-1 avec pour conséquence la jolie formule $\mathrm{pgcd}(a^n-1, a^m-1) = a^{\mathrm{pgcd}(m,n)}-1$.

q3) On a $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\dots+1)$ et les deux facteurs sont supérieurs stricts à 1 donc pour $a>2$, $n>1$, a^n-1 est divisible par $a-1 \neq 1$, $a-1 \neq a^n-1$ et il n'est pas premier.

q4) Si $n=ml$, $m,l \in \mathbb{N}$, $m>1$, $l>1$ alors d'après q2) on a que $2^m-1 \mid 2^n-1$ (et $2^l-1 \mid 2^n-1$) avec $2^m-1 \neq 1$ et $2^m-1 \neq 2^n-1$. Alors 2^n-1 ne peut pas être premier.

Par conséquent si 2^n-1 est premier, obligatoirement n est premier.

Ex 10 q1) On a $7777 \equiv 7 \equiv -3$ [10] donc $7777^{7777} \equiv (-3)^{7777}$ [10]

Or $(-3)^2 \equiv 9 \equiv -1$ [10] donc $(-3)^4 \equiv 1$ [10] donc $(-3)^{4k} \equiv 1^k \equiv 1$ [10] pour $k \in \mathbb{Z}$

Mais $7777 \equiv 1$ [4] donc $7777 = 4k+1$ avec $k \in \mathbb{Z}$.

Par conséquent $7777^{7777} \equiv (-3)^{4k+1} \equiv (-3)^{4k}(-3)$ [10] Finalement

$7777^{7777} \equiv 1 \cdot (-3) \equiv -3 \equiv 7$ [10]

donc le dernier chiffre de 7777^{7777} est 7.

q2) On a $900 \equiv 3$ [13] donc $900^{2000} \equiv 3^{2000}$ [13]. On remarque que $3^3 \equiv 1$ [13] et que $2000 \equiv 2$ [3]. Par conséquent $3^{2000} \equiv (3^3)^{666} \cdot 3^2 \equiv 9$ [13] donc $900^{2000} \equiv 9 \equiv -4$ [13].

On a $101 \equiv 10$ [13] et $101 \equiv (-3)$ [13]. Donc comme $(-3)^6 \equiv 1$ [13] et que $102 \equiv 0$ [6] d'où $102^{103} \equiv 0$ [6] on a que $101^{102^{103}} \equiv (-3)^{6k} \equiv 1^k \equiv 1$ [13].

93) On a $31 \equiv 3\ [7]$ et $3^3 \equiv -1\ [7]$ donc $3^6 \equiv 1\ [7]$.

On a $32 \equiv 2\ [6]$ donc $32^{33} \equiv 2^{33}\ [6]$.

Or $2^2 \equiv -2\ [6]$ et $2^3 \equiv 2\ [6]$. On pense alors à démontrer par récurrence que

$P_n : 32^n \equiv (-1)^{n+1} \cdot 2\ [6]$. On a vu que P_1 était vrai.

Si P_n est vraie alors $32^{n+1} \equiv 32 \cdot 32^n \equiv 2 \cdot (-1)^{n+1} \cdot 2\ [6]$

donc $32^{n+1} \equiv (-1)^{n+1}(-2)\ [6]$ d'où $P_{n+1} : 32^{n+1} \equiv (-1)^{n+2} \cdot 2\ [6]$.

La propriété de récurrence est donc vraie.

Alors $32^{33} \equiv 2\ [6]$ donc $32^{33} = 6k+2$.

Finalement $31^{32^{33}} \equiv 3^{6k+2} \equiv (3^6)^k \cdot 3^2 \equiv 1 \cdot 9 \equiv 9 \equiv 2\ [7]$.

94) On a $100 \equiv 4\ [12]$ et $4^2 \equiv 4\ [12]$ donc $4^n \equiv 4\ [12]\ \forall n \geq 1$ en procédant de nouveau par récurrence : soit P_n la propriété de récurrence $4^n \equiv 4\ [12]$. On a P_1 vraie et si P_n est vraie alors $4^{n+1} \equiv 4 \cdot 4 \equiv 4\ [12]$ donc P_{n+1} est vraie. Ceci conclut le raisonnement par récurrence. Conclusion $100^{100^{100}} \equiv 4^{100^{100}} \equiv 4\ [12]$.

ex11 On a $5 \equiv -2\ [7]$ et $12 \equiv -2\ [7]$.

Or $2^3 \equiv 1\ [7]$ et $(-2)^3 \equiv -1\ [7]$ donc $(-2)^6 \equiv 1\ [7]$.

On a que $6614 \equiv 2\ [6]$ et que $857 \equiv 5\ [6]$ donc

$5^{6614} \equiv (-2)^{6k+2} \equiv (-2)^{6k}(-2)^2 \equiv 4\ [7]$ et

$12^{857} \equiv (-2)^{6l+5} \equiv (-2)^{6l}(-2)^5 \equiv (-2)^3(-2)^2 \equiv -4 \equiv 3\ [7]$.

Au total $5^{6614} - 12^{857} \equiv 1\ [7]$.

ex12 a) On voit facilement que 4 est un inverse de 2 modulo 7 car $4 \times 2 \equiv 8 \equiv 1\ [7]$. Alors $2x \equiv 1\ [7] \iff 4 \cdot 2x \equiv 4\ [7] \iff 8x \equiv 4\ [7] \iff x \equiv 4\ [7]$, solution de notre équation.

b) $4x \equiv 6\ [18] \iff 4x = 6 + 18k,\ k \in \mathbb{Z} \iff 2x = 3 + 9k,\ k \in \mathbb{Z}$

$\iff 2x \equiv 3\ [9]$. Comme 5 est un inverse de 2 modulo 9 car

$5 \times 2 = 10 \equiv 1\ [9]$ on a $2x \equiv 3\ [9] \iff 5 \times 2x \equiv 15 \equiv 6\ [9]$

$\iff 10x \equiv 6\ [9] \iff x \equiv 6\ [9]$, solution de notre équation.

c) $12x \equiv 9\ [6] \iff 12x = 9 + 6k,\ k \in \mathbb{Z}$. Or pgcd$(6,12) = 6 \nmid 9$

donc cette équation n'admet pas de solutions dans $\mathbb{Z}$.

d) $23x \equiv 41 \mod 52$ admet des solutions car pgcd$(23,52) = 1$.

Il faut chercher un inverse de 23 modulo 52. Ceci se fait à l'aide d'une relation de Bezout entre 23 et 52. Une telle relation s'obtient en remontant l'algorithme d'Euclide entre 52 et 23 c.à.d :

$52 = 23 \times 2 + 6$; $23 = 6 \times 3 + 5$; $6 = 5 \times 1 + 1$ d'où

$1 = 6 - (23 - 6 \times 3) = 6 \times 4 - 23 = (52 - 23 \times 2) \times 4 - 23 = 52 \times 4 + 23 \times (-9)$

Alors -9 est un inverse de 23 modulo 52 car $23 \times (-9) \equiv 1\ [52]$.

On a $23x \equiv 41\ [52] \iff -9 \times 23\, x \equiv -9 \times 41\ [52] \iff x \equiv -369\ [52]$

$\iff x \equiv -5\ [52]$ (f) $5x \equiv -1\ [8] \iff 3 \cdot 5x \equiv -3\ [8] \iff -x \equiv -3\ [8] \iff x \equiv 3\ [8]$

e) $68x \equiv 100\ [120] \iff 68x = 100 + 120k,\ k \in \mathbb{Z} \iff 17x = 25 + 30k,\ k \in \mathbb{Z}$

$\iff 17x \equiv 25\ [30]$ qui admet des solutions car pgcd$(17,30) = 1$.

On cherche l'inverse de 17 modulo 30 en utilisant de nouveau l'algorithme d'Euclide et la relation de Bezout qui en découle :

$30 = 17 + 13$, $17 = 13 + 4$, $13 = 4 \times 3 + 1$ donc $1 = 13 - 4 \times 3 = 13 - (17 - 13) \times 3 =$

$= 13 \times 4 - 17 \times 3 = (30 - 17) \times 4 - 17 \times 3 = 30 \times 4 - 17 \times 7$. Donc -7 est un inverse de 17 modulo 30, vu que $-7 \times 17 \equiv 1\ [30]$. Alors $17x \equiv 25\ [30] \iff$

$-7 \times 17\, x \equiv -7 \times 25\ [30] \iff x \equiv (-7)(-5)\ [30] \iff x \equiv 35\ [30] \iff x \equiv 5\ [30]$.

(g) $20x \equiv 4\ [30]$ n'a pas de solutions car pgcd$(20,30) = 10 \nmid 4$. (h) Pas de sol car pgcd$(20,4) = 4 \nmid 30$

Ex 13) L'idée est la même que ci-dessus, vu que $\overline{171}\, x = \overline{7} \iff 171x \equiv 7\ [212]$

On cherche donc un inverse de 171 modulo 212, c.à.d l'inverse de $\overline{171}$ dans $\mathbb{Z}/212\mathbb{Z}$. On a $212 = 171 \times 1 + 41$, $171 = 41 \times 4 + 7$, $41 = 7 \times 5 + 6$, $7 = 6 \times 1 + 1$

donc $1 = 7 - 6 = 7 - (41 - 7 \times 5) = 7 \times 6 - 41 = (171 - 41 \times 4) \times 6 - 41 = 171 \times 6 - 41 \times 25 =$

$= 171 \times 6 - (212 - 171) \times 25 = 171 \times 31 - 212 \times 25$. Donc $31 \cdot 171 \equiv 1\ [212]$

et 31 est un inverse de 171 modulo 212 (ceci a été possible car pgcd$(171,212) = 1$)

ou encore $\overline{171}^{-1} = \overline{31}$ dans $\mathbb{Z}/212\mathbb{Z}$ car $\overline{171} \cdot \overline{31} = \overline{1}$. Alors $\overline{171}\, x = \overline{7}$

$\iff \overline{31} \cdot \overline{171}\, x = \overline{31} \cdot \overline{7} = \overline{5} \iff x = \overline{5}$ dans $\mathbb{Z}/212\mathbb{Z}$.